МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования
ТИХООКЕАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра Экономической кибернетики

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Задание и методические указания к контрольной работе для студентов заочного отделения

Специальность – «Прикладная информатика в экономике»

Хабаровск, 2011

Введение

Расчетный объем дисциплины «Информационная безопасность» по кафедре «Экономическая кибернетика» для студентов заочного отделения специальности «Прикладная информатика в экономике» составляет 187 часов, включая 16 часов аудиторных занятий и 171 часов самостоятельной работы. Аудиторные занятия проводятся в университете в период сессии по расписанию, самостоятельную работу студент выполняет в течение периода, предшествующего сессии, по своему индивидуальному плану. В процессе изучения студент должен выполнить и защитить контрольную работу, пройти тест в адаптивной системе контроля качества знаний и сдать экзамен.

При изучении дисциплины «Информационная безопасность» студенты-заочники должны использовать данное методическое пособие, включая рабочую программу, методические указания и контрольные задания. Кроме того, они должны использовать предоставляемые кафедрой в электронном варианте средства программного и информационного обеспечения для записи на носитель данных студента, а также основную и дополнительную литературу.

I. РАБОЧАЯ ПРОГРАММА ПО ДИСЦИПЛИНЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» ДЛЯ СТУДЕНТОВ ЗАОЧНОГО ОТДЕЛЕНИЯ СПЕЦИАЛЬНОСТИ «ПРИКЛАДНАЯ ИНФОРМАТИКА В ЭКОНОМИКЕ»

Рабочая программа состоит из списка рекомендуемой литературы и наименований разделов программы с описанием их содержания.

В круглых скобках рядом с названием раздела указано количество часов самостоятельной работы.

В квадратных скобках после каждого раздела указана рекомендуемая для его изучения литература, причем учебные пособия обозначаются своими порядковыми номерами в следующем далее списке.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

<u>Основная</u>

1. Галатенко В.А. Основы информационной безопасности. - М. : Интернет-Ун-т Информ.Технологий, 2004 .- 263с.
2. Галицкий А.В. Защита информации в сети – анализ технологий и синтез решений.-М.,2004.
3. Корт С.С. Теоретические основы защиты информации.-М.,2004.
4. Основы информационной безопасности.-М.,2006.
5. Основы организационного обеспечения информационной безопасности объектов информатизации.-М.,2005.
6. Семененко В.А. Информационная безопасность.-М.,2005.

Дополнительная

7.Гринберг А.С. и др. Защита информационных ресурсов государственного управления.-М.,2003.
8.Малюк А.А. и др. Введение в защиту информации в автоматизированных системах.-М.,2001.
9.Соколов А.В. Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах.-М.,2002.

НАИМЕНОВАНИЯ РАЗДЕЛОВ ДИСЦИПЛИНЫ, ИХ СОДЕРЖАНИЕ С УКАЗАНИЕМ ЛИТЕРАТУРЫ И ОБЪЕМА В ЧАСАХ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТА-ЗАОЧНИКА

Введение

Общая характеристика состояния и развития теории информационной безопасности как совокупности знаний. Место и роль учебной дисциплины в овладении студентами знаниями, умениями и навыками, необходимыми им в профессиональной деятельности, место дисциплины в межпредметных логических связях.
[1-9]

Основные понятия и принципы информационной безопасности

Понятие информационной безопасности. Защита информации. Основные механизмы безопасности.

Ценность информации как фактор, требующий ее защиты в рыночной экономике. Основные понятия ИБ. Конфиденциальность, целостность, достоверность, юридическая значимость информации. Целостность ресурса или компонента системы.

Основы построения защищенных ЭИС: защищенные коды экономической информации.

Угрозы безопасности для информационной системы. Классификация угроз и их основные особенности. Характеристика угроз безопасности с использованием данных статистики и результатов анализа функционирования современных систем.

Основные понятия ИБ. Политика безопасности. Атаки на информационные ресурсы: классификация, методы и технология. Принципы защиты информации от несанкционированнного доступа. Модели ИБ и защита информации, политика защиты информационных ресурсов.
[1-9]

Основные нормативные материалы по информационной безопасности

Общая характеристика нормативно-правовых основ ИБ.

Сертификация и стандартизация в процессе защиты информационных ресурсов.

Нормативные документы по защите информации.

Стандарты ГОСТ.

Стандарты ISO.

[7]

Принципы организации подсистемы информационной безопасности

Internet, электронный бизнес и основные проблемы безопасности КИС.

Модель угроз безопасности КИС.

Модель противодействия угрозам безопасности КИС.

Принципы и методы построения подсистемы информационной безопасности КИС.

Методы адаптивного управления информационной безопасностью.

[1,9]

Методы криптографии

Введение в криптографическую защиту информации. Основные понятия и определения.

Классификация средств криптографической защиты информации.

Симметричные криптосистемы. Основные понятия. Классическая сеть Фейстеля. Блочные алгоритмы шифрования данных.

Асимметричные криптосистемы. Основные понятия. Модель асимметричной RSA-криптосистемы. Процедуры шифрования и расшифрования в RSA-криптосистеме.

Отечественный стандарт шифрования данных. Стандарты DES и AES.

Основные свойства и процедуры электронной цифровой подписи. Принципы построения системы электронной цифровой подписи RSA. Характеристика основных процедур системы электронной цифровой подписи RSA.

Идентификация и аутентификация. Основные понятия и классификация средств и процессов.

[1-9]

Технологии защиты информационных ресурсов в ЭИС

Методы использования форматированных сообщений и макетов в распределенных системах сбора и обработки экономической информации.

Методы и средства защиты информации в MS SQL Server.

Характеристика уязвимостей КИС по уровням ее стандартной организации: Excel и MS Query; MS SQL Server и Access; Windows NT; TCP/IP.

Особенности политики безопасности в Windows2000 и WindowsXP. Управление доступом при работе с прикладными программами.

Свойства Internet Explorer.

Характеристика комплекса стандартов IPSec.

Компьютерные вирусы как специальный класс самопродуцирующихся программ. Классификация вирусов. Средства антивирусной защиты.

Методы организации защищенных ЭИС на основе использования технологий защиты информационных ресурсов. Концепция построения виртуальных частных сетей VPN. Туннелирование.

Функции и компоненты сети VPN. Средства VPN.

Варианты построения защищенных каналов VPN.

Сервисы безопасности сети VPN.

Классификация виртуальных частных сетей VPN.

Основные варианты VPN-решений для построения защищенных корпоративных систем. VPN на базе сетевых операционных систем. VPN на базе маршрутизаторов. VPN на базе межсетевых экранов.

VPN – продукты ЗАСТАВА.

Протокол SOCKS. Функции SOCKS – сервера.

Способы защиты информации в технологиях ISDN и Frame Relay. Средства X.25 – сетей.

[1-9]

2 ЗАДАНИЕ И МЕТОДИЧЕСКИЕ УКАЗАНИЯ

Задание 1

Определить угрозы информационной безопасности на основе качественного анализа уязвимостей используемых ИТ и функционирующих ИС. Охарактеризовать угрозы по видам нарушения безопасности информации, по природе происхождения, предпосылкам появления и источникам угроз. Там, где это необходимо, определить каналы несанкционированного получения информации.

Задачи

1. Выполнить анализ уязвимостей и определить угрозы информационной безопасности для процесса обмена информацией:

- через городскую телефонную сеть с установкой модемов на номерах АТС;
- через специально оборудованную кабельную линию связи;
- через Internet;

если при этом осуществляется:

- передача сообщений в виде полносвязного текста;
- передача форматированных сообщений при использовании сетевого системного и прикладного программного обеспечения;
- передача форматированных сообщений при использовании специально разработанных макетов.

2. Выполнить анализ уязвимостей и определить угрозы информационной безопасности для пользователей локальной сети офиса, взаимодействующих с Internet:

0) при размещении сообщений на собственном сайте и в других узлах;
1) при использовании электронной почты;
2) при поиске информации в Web-среде;
3) при «скачивании» файлов;
4) при передаче форматированных сообщений на определенный сайт;
5) при передаче документов, содержащих SQL-запросы;
6) при работе с корпоративной базой данных и знаний в режиме дистанционного доступа;
7) при использовании системы электронной коммерции;
8) при работе в РТС;
9) при использовании прикладным программным обеспечением внешнего источника информации. Рассмотреть протоколы TCP/IP и IPSec. Номер варианта соответствует последней цифре шифра студента.

3. Выполнить анализ уязвимостей и определить угрозы информационной безопасности в ИС для пользователей локальной сети офиса, осуществляющих:

1) ввод первичных документов путем заполнения всех полей форм существующих бланков;
2) ввод текстовых документов с использованием сканера;
3) ввод форматированных документов оперативного учета с использованием сканера;
4) ввод данных с переданной дискеты;
5) корректировку базы данных в локальной сети с выделенным сервером;
6) поиск информации в корпоративной сети;
7) запуск программ с помощью графического пользовательского интерфейса;
8) запуск программ с помощью командного интерфейса;
9) доступа к информации с помощью драйвера ODBC;

0) обновление данных с использованием механизмов DDE.

Номер варианта соответствует последней цифре шифра студента.

4. Выполнить анализ уязвимостей и определить угрозы информационной безопасности в ИС, если информация подсистемы управления проектами выводится:

- на монитор;
- на принтер;
- на жесткий диск;
- на дискету;

при этом в помещении офиса могут находиться (кроме сотрудников организации):

- инженер-электроник организации;
- программист организации;
- консультант по бизнес-решениям из внешней организации;
- любой работник организации;
- любой посетитель;
- специалист по программным средствам управления проектами;
- уборщица;

при этом электропитание аппаратных средств осуществляется:

- от внешнего источника энергоснабжения без использования УБП;
- от внешнего источника энергоснабжения с использованием УБП.

5. Выполнить анализ уязвимостей и определить угрозы информационной безопасности в ИС для следующих ситуаций:

1) в прикладной программе количество пунктов и параметров подчиненных меню больше 12;
2) пакет прикладных программ экономического назначения является функционально замкнутым;
3) пакет прикладных программ экономического назначения разработан для фиксированного состава документов;
4) состав АРМ и модулей корпоративной системы не соответствует организационной структуре отдела;
5) пользователи автономных АРМ передают друг другу общие данные на дискетах;
6) пакет прикладных программ обеспечивает автоматизацию одного раздела бухгалтерского учета;
7) отношения в составе базы данных представлены во второй нормальной форме;
8) структура базы данных обладает цикличностью;
9) в пакете прикладных программ используется доступ по номеру записи на основе индексной таблицы;
0) в структуре кодового обозначения отсутствует контрольное число.

Номер варианта соответствует последней цифре шифра студента.

Методические указания по выполнению задания 1

Угроза информационной безопасности – любое потенциально возможное событие, которое может нанести ущерб информации и поддерживающей ее инфраструктуре и, вследствие этого, быть причиной экономического ущерба для организации в настоящее время или в будущем.

Ущерб информации оценивается также степенью ухудшения ее качественных характеристик: достоверности, целостности, актуальности, своевременности, ценности, актуальной полезности, конфиденциальности , полноты, критичности.

По природе происхождения угрозы могут быть случайными (отказы, сбои, ошибки в проектах и программах, стихийные бедствия, побочные влияния), а также – преднамеренными (злоумышленные действия людей).

Существуют предпосылки появления угроз различной природы: объективные (количественная и качественная недостаточность составных частей и элементов ИС, в том числе, функциональной части, информационного, программного, математического, технического, организационного, эргономического, лингвистического, методического, кадрового, правового обеспечения), а также субъективные (деятельность разведорганов иностранных государств, промышленный шпионаж, уголовные элементы, психически ненормальные люди, недобросовестные или неквалифицированные сотрудники, недобросовестные или неквалифицированные разработчики). Недостаточность ИС как объективная предпосылка возникновения угроз чаще всего объясняется недостаточностью теории ИС, средств проектирования и программирования, технических средств.

При наличии предпосылок появления угрозы могут поступать от различных источников. В качестве таких источников могут выступать: 1) люди (посторонние юридические и физические лица, пользователи и все сотрудники организации, включая персонал ИС, а также разработчики и все продавцы программных продуктов и документации); 2) технические устройства (средства сбора и регистрации, передачи, ввода, обработки, хранения и выдачи информации); 3) модели, алгоритмы, программы, реализованные в программных средствах общего назначения и в прикладных программах; 4) технологические схемы обработки данных (ручные, интерактивные, внутримашинные, сетевые); 5) внешняя среда (состояние атмосферы, побочные сигналы, влияния и воздействия).

В результате реализации угроз из различных источников могут иметь место различные виды нарушений информационной безопасности:

уничтожение данных или нарушение целостности информации; искажение логической структуры данных; искажение содержания сообщений вследствие их модификации и подмены; нарушение конфиденциальности информации вследствие несанкционированного доступа; хищение информации; хищение программных и технических средств; уничтожение или нарушение нормальной работы программных и технических средств; несвоевременное поступление информации.

Теория надежности автоматизированных систем изучает причины появления и действие угроз случайной природы с объективными предпосылками возникновения. Теория информационной безопасности изучает эти же угрозы в единстве с преднамеренными, учитывает общий ущерб от реализации всех угроз и рассматривает информационные системы не только на стадии эксплуатации, но и на всех остальных стадиях жизненного цикла. Она является теоретической базой создания подсистемы информационной безопасности, организации адаптивного управления информационной безопасностью.

При анализе преднамеренных угроз рассматривают каналы несанкционированного получения информации, подразделяя их на 6 классов. Каналы первого класса возникают и существуют безотносительно к обработке информации и без доступа злоумышленника к элементам системы. Они также называются общедоступными постоянными каналами. Сюда относят подслушивание разговоров и хищение данных на носителях за пределами офиса. Каналы второго класса возникают и существуют в процессе обработки информации и без доступа злоумышленника к элементам системы. Современная аппаратура позволяет дистанционно прослушивать все линии передачи данных, в том числе высокоскоростные, осуществлять перехват и дешифрацию сообщений. Каналы третьего класса возникают и существуют безотносительно к обработке информации и с доступом злоумышленника к элементам системы без изменения последних. Здесь рассматривают копирование информации. Каналы четвертого класса возникают и существуют в процессе обработки информации и с доступом злоумышленника к элементам системы без изменения последних. Сюда чаще всего относят незаметное копирование информации из компьютера в процессе использования игровых и деловых программ, которые содержат замаскированные подпрограммы, позволяющие контролировать весь компьютер. Каналы пятого класса возникают и существуют безотносительно к обработке информации с доступом злоумышленника к элементам системы с изменением последних. Каналы шестого класса возникают и существуют в процессе обработки информации с доступом злоумышленника к элементам системы с изменением последних /8, с.22-27/.

Задание 2

Определить вероятность несанкционированного получения информации. Записать все расчетные формулы, развернутые расчеты и анализ их результатов.

Задачи

1. В рассматриваемой ЭИС возможны нарушители двух категорий – внешние и внутренние. В качестве компонентов, являющихся объектами несанкционированных действий, рассматриваются дискеты, дисплеи и принтеры. Каналами несанкционированного получения информации являются кражи дискет и машинограмм (распечаток), незаметный просмотр информации при ее выводе пользователями на дисплеи и на принтеры.

Конфигурацию и все соответствующие вероятности определить самостоятельно (собственный вариант). Также самостоятельно определить зоны и каналы несанкционированного получения информации.

Определить вероятность несанкционированного получения информации нарушителем определенной категории по определенному каналу несанкционированного получения информации в зоне определенного структурного компонента ИС. Рассмотреть все возможные случаи и ситуации. Записать все расчетные формулы, развернутые расчеты и анализ их результатов.

2. В рассматриваемой ЭИС возможны внутренние нарушители. В качестве компонентов, являющихся объектами несанкционированных действий, рассматриваются жесткие диски, дискеты, дисплеи и принтеры. Каналами несанкционированного получения информации являются кражи дискет и машинограмм (распечаток), незаметный просмотр информации при ее выводе пользователями на дисплеи и на принтеры, несанкционированный доступ к базе данных и копирование информации при временном отсутствии пользователей на рабочих местах.

Конфигурацию и все соответствующие вероятности определить самостоятельно (собственный вариант). Также самостоятельно определить зоны и каналы несанкционированного получения информации.

Определить вероятность несанкционированного получения информации нарушителем определенной категории по определенному каналу несанкционированного получения информации в зоне определенного структурного компонента ИС. Рассмотреть все возможные случаи и ситуации. Записать все расчетные формулы, развернутые расчеты и анализ их результатов.

Методические указания по выполнению задания 2

Для определения вероятности несанкционированного получения информации нарушителем определенной категории по определенному каналу несанкционированного получения информации в зоне определенного структурного компонента ИС рекомендуется использовать формулу, приведенную в учебнике /8/:

$$P_{ijkl} = P_{ikl}^{дос} P_{ijl}^{кан} P_{ijkl}^{п} P_{ijl}^{и} \qquad (1)$$

Здесь

$P_{ikl}^{дос}$ - вероятность доступа нарушителя k-ой категории в l-ую зону i-ого компонента;

$P_{ijl}^{кан}$ - вероятность возникновения и существования j-ого канала несанкционированного получения информации в l-ой зоне i-ого компонента;

$P_{ijkl}^{п}$ - вероятность доступа нарушителя k-ой категории к j-му каналу несанкционированного получения информации в l-ой зоне i-ого компонента;

$P_{ijl}^{и}$ - вероятность наличия защищаемой информации в j-ом канале несанкционированного получения информации в l-ой зоне i-ого компонента в момент доступа туда нарушителя.

Задание 3

Изучить основные особенности организации и функционирования симметричных криптосистем теоретически и на конкретном материале.

Разработать принципиальную схему и описание модели симметричной криптосистемы для обмена секретной информацией в организации и между произвольными корреспондентами. С использованием типовой принципиальной схемы и примера ее применения решить задачу организации системы путем сопоставления вариантов.

Задачи

1. На основе применения приведенных в методических указаниях формул по использованию совершенного шифра в симметричной криптосистеме выполнить процедуры шифрования и расшифрования

собственной фамилии. Составляющие ключа выбрать произвольно в соответствии с требованиями методики.

2. Разработать принципиальную схему и описание модели симметричной криптосистемы для обмена секретной информацией в организации и между произвольными корреспондентами. С использованием типовой принципиальной схемы и примера ее применения решить задачу организации системы путем сопоставления вариантов.

Методические указания по выполнению задания 3

Шифр – совокупность инъективных отображений множества открытых текстов во множество шифрованных текстов, проиндексированная элементами из множества ключей:

$$\{E_k: M \rightarrow C,\ k \in K\} \qquad (2)$$

Здесь

M – множество возможных открытых текстов;

C - множество шифрованных текстов (криптограмм);

K - множество ключей.

Для того, чтобы зашифровать сообщение $m \in M$, необходимо выбрать ключ $k \in K$ и применить к m отображение E_k. Результат такого применения $c = E_k(m)$ является результатом шифрования текста m на ключе k. Для расшифрования используется отображение D_k:

$$\{D_k: C \rightarrow M,\ k \in K\} \qquad (3)$$

Результат такого применения $m = D_k(c)$ является результатом расшифрования текста c на ключе k.Заметим, что инъективным называется отображение множества A во множество B, при котором различные элементы из A имеют различные образы в B. Ключ выбирается случайно из некоторого вероятностного распределения на множестве K. Для обеспечению максимальной стойкости системы к дешифрованию стараются обеспечить случайный равновероятный выбор. Многие авторы для строгости изложения материала указывают, что расшифрование по известному ключу осуществляется на стороне приемника сообщения, а дешифрование по неизвестному ключу выполняет злоумышленник, перехвативший сообщение (прослушивающий канал связи).

Шифры называют совершенными, если они не поддаются расшифрованию ни при каких условиях. Определение совершенного шифра дано К.Шенноном: это шифр, при использовании которого перехват

криптограммы не дает противнику никакой информации, даже если он обладает неограниченными вычислительными ресурсами. В этом случае, если открытый текст $m \in M$ состоит из n символов, ключ k тоже должен состоять из n чисел k_1 ,.., k_n ,складываемых по модулю N с числами, соответствующими (логически эквивалентными) символам открытого текста.

Поскольку ключ $k \in K$ выбирается случайно и равновероятно, шифр называют шифром гаммирования со случайной равновероятной гаммой.

Приведем пример такого шифра. Пусть открытый текст $m \in M$ длиной из n символов состоит из букв $m_1 \ldots m_n$ алфавита A из 32 букв русского языка и пробела. Ключ $k \in K$ представляет собой последовательность чисел k_1 ,.., k_n из множества чисел $V = \{0,1,\ldots,32\}$, представляющих собой номера букв в . алфавите A. Пусть определена функция $F(m_i)$, отображающая символ m_i в его порядковый номер. Тогда числа зашифрованного текста c_1 ,.., c_n можно определить по формуле:

$$c_i = (F(m_i) + k_i) \bmod 33 \qquad (4)$$

Запись $d=(a+b) \bmod N$ означает, что d равен остатку от деления на N суммы $(a+b)$, например, 2=(6+7) mod 11.

Пусть определена функция $G(F(m_i))$, отображающая порядковый номер символа в собственно символ m_i. Тогда открытый текст $m \in M$ из букв $m_1 \ldots m_n$ посимвольно можно получить по формуле:

$$m_i = G((c_i + (33 - k_i)) \bmod 33) \qquad (5)$$

Поскольку на стороне источника информации и на стороне приемника используется один и тот же ключ, применяемый для шифрования отправителем сообщения m и для расшифрования получателем шифртекста c, рассматриваемая криптосистема является симметричной.

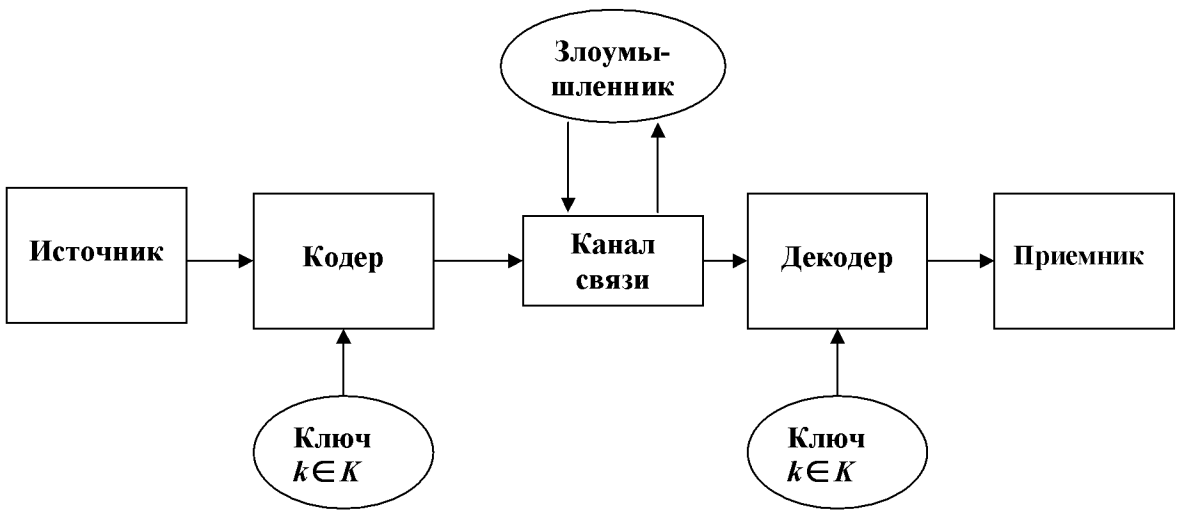


Рис. 1 Принципиальная схема симметричной криптосистемы

Таким образом, при использовании в симметричной криптосистеме совершенного шифра обеспечивается полная защита от несанкционированного доступа при перехвате сообщения (при прослушивании канала).

Целостность сообщения обеспечивается только смысловой интерпретацией его содержания на стороне приемника.

Задание 4

Изучить основные особенности организации и функционирования асимметричных криптосистем теоретически и на конкретном материале.

Изучить и выполнить процедуры определения секретных чисел и ключей, а также шифрования и расшифрования для асимметричных криптосистем. С использованием изученных элементов математического аппарата и принципиальной схемы асимметричной криптосистемы последовательно выполнить указанные операции.

Номер варианта соответствует последней цифре шифра студента.

Задачи

1. В RSA-системе разложите на простые множители число n и определите φ. Запишите расчетные формулы.

Дайте оценку применения такой процедуры злоумышленником.

Таблица 1

Номер варианта	n
0	221
1	391
2	817
3	437
4	493
5	407
6	517
7	667
8	1147
9	713

2. Зашифруйте сообщение на открытом ключе K_1 =7, n=33. Исходное сообщение состоит из числовых кодовых обозначений (от 0 до 32), которыми закодированы буквы русского алфавита и пробел из открытого сообщения.

Определите параметры асимметричной криптосистемы, которые отсутствуют в описании задачи, и выполните процедуру расшифрования до получения открытого текста.

Таблица 2

Номер варианта	Открытое сообщение
0	ВИРУС ПТИЧЬЕГО ГРИППА
1	СЕРТИФИКАТ БЕЗОПАСНОСТИ
2	ЗАЩИТА ИНФОРМАЦИИ
3	КОНТРОЛЛЕР ЖЕСТКОГО ДИСКА
4	ТРАФИК ПЕРЕДАЧИ ДАННЫХ
5	ТУННЕЛИРОВАНИЕ ЧЕРЕЗ ШЛЮЗ
6	ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ
7	ОПЕРАЦИОННАЯ СИСТЕМА
8	ДОСТУП ПО КЛЮЧУ
9	НЕСАНКЦИОНИРОВАННЫЙ

1. Разработайте принципиальную схему обмена текстовыми документами, заверенными электронной цифровой подписью, между двумя абонентами (с передачей в прямом и обратном направлениях).

Методические указания по выполнению задания 4

В асимметричной криптосистеме на стороне источника и на стороне приемника используются различные ключи. Для шифрования используется один ключ, а для расшифрования – другой. Эти ключи связаны и взаимно определяют друг друга. Для их формирования используется генератор ключей.

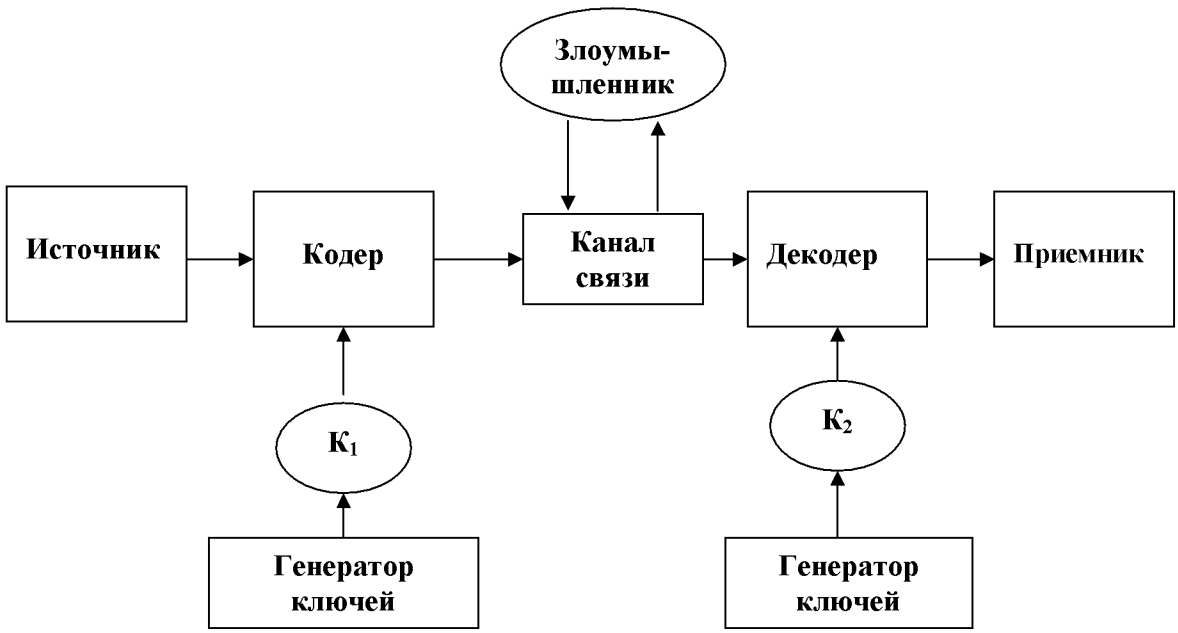


Рис. 3 Принципиальная схема асимметричной криптосистемы

При генерации используются большие числа P и Q (порядка 2^{526}). Они являются секретными. Процедуры шифрования и расшифрования связаны с вычислением выражений по модулю N. Для определения N используется формула:

$$N = P*Q \qquad (6)$$

Ключи K_1 и K_2 определяют следующим образом. Сначала вычисляют значение φ:

$$\varphi = (P - 1)*(Q - 1) \qquad (7)$$

Затем находят K_1 и K_2 из соотношения:

$$K_1*K_2 \equiv 1 \ mod \ \varphi \qquad (8)$$

Если $P=3$, а $Q=11$, тогда $N=33$, а $\varphi=20$. В этом случае $K_1=3$, а $K_2=7$ (или наоборот). Ключ K_1 используется на стороне источника для шифрования, ключ K_2 – на стороне приемника для расшифрования. Функция для шифрования записывается следующим образом:

$$\tilde{n}_i = E_{K_1}(m_i), \quad m \in M \qquad (9)$$

$$c_i = (m_i^{K_1}) \ mod \ N \qquad (10)$$

Функция для расшифрования в асимметричной криптосистеме определяется следующим образом:

$$m_i = D_{K_2}(c_i) \qquad (11)$$

$$m_i = (c_i^{K_2}) \ mod \ N \qquad (12)$$

Асимметричные криптосистемы используются, в основном, при взаимодействии пользователей, тогда как симметричные – при взаимодействии технических средств в сетях передачи данных.

Существует метод дешифрации для рассмотренной асимметричной криптосистемы. Он связан с определением секретных чисел P и Q ,если

удалось узнать значение N. После определения значений P и Q открывается возможность нахождения ключей K_1 и K_2. Поэтому надо разложить на простые сомножители целое число N. Чтобы задача стала практически неразрешимой при генерации используются большие числа P и Q (порядка 2^{526}). Кроме того, что они выбираются случайным образом, они еще находятся в значительном удалении по отношению друг к другу.

Покажем, что произойдет, если числа P и Q будут небольшими и достаточно близкими друг другу. Вместе с этим оценим трудоемкость процедуры дешифрации. Если $P > Q$, тогда для величин $X=(P+Q)/2$ и $Y=(P-Q)/2$ справедливо соотношение

$$X^2 - Y^2 = PQ = N \qquad (13)$$

Данное уравнение имеет единственное решение, а N единственным образом раскладывается на простые сомножители. Рассматривая выражение $X^2 - N = Y^2$, и перебирая в порядке возрастания варианты $X > \sqrt{N}$, вычисляя при этом Y, можно найти решение уравнения.

Например, если $N=851$, установим $X=30$ и получим $Y=7$. Отсюда $P=37$, $Q=23$.

Задание

Разработать принципиальную схему решения по защите информации в организации, функционирующей на основе корпоративной или локальной сети и Internet.

На основе типового структурного представления организации («центральный офис – филиалы – удаленные структурные подразделения – точки взаимодействия»), рассмотренной среды передачи и обработки информации разместить серверы, центры управления, центры сертификации, межсетевые экраны, персональные сетевые экраны, хостовые и сетевые сенсоры, коммутаторы, криптошлюзы, датчики антивирусной защиты, средства защиты от спама, сетевые и серверные датчики системы обнаружения вторжений, агенты системы защиты от утечки информации, маршрутизаторы, карт-ридеры, рабочие станции. Определить компоненты решения и выбрать соответствующие программные продукты.

Номер варианта соответствует последней цифре шифра студента.

Задачи

1.Разработать решение по защите информационной системы банка.

2.Разработать решение по защите информационной системы завода отопительного оборудования.
3.Разработать решение по защите информационной системы проектного института.
4. Разработать решение по защите информационной системы фондовой биржи.
5.Разработать решение по защите информационной системы страховой компании.
6.Разработать решение по защите информационного взаимодействия в сети супермаркетов.
7.Разработать решение по защите информации в коммерческой структуре, включающей главный офис, 2 филиала, 5 магазинов, 2 склада.
8.Разработать решение по защите информации в региональном статистическом управлении.
9. Разработать решение по защите информации в коммерческой структуре, включающей главный офис, 1 филиал, 3 магазина, 4 склада.
0.Разработать решение по защите информации в коммерческой структуре, включающей главный офис, 8 магазинов, 1 склад.

Методические указания по выполнению задания 5

Процесс внедрения комплексного решения предусматривает несколько этапов, отображённых на приведенном ниже рисунке. На первом из них компания проводит комплекс работ по обследованию текущего состояния информационной безопасности автоматизированной системы Заказчика. Полученные результаты являются основой для работ по адаптации решения с учётом специфики защищаемой системы. Процедура адаптации включает в себя уточнение состава решения, а также разработку схемы размещения и конфигурации подсистем защиты. Кроме того проводится разработка проектных решений по защите от угроз безопасности, а также готовится рабочая и техническая документация на создаваемый комплекс безопасности.

Следующий этап работ предполагает обучение персонала Заказчика вопросам, связанным с эксплуатацией системы защиты. Процесс обучения включает как теоретические, так и практические аспекты защиты информации.

На завершающем этапе проводятся работы по внедрению и техническому сопровождению комплексной системы защиты. По завершению пуско-наладочных работ проводятся стендовые испытания установленных средств защиты и разрабатывается пакет организационно-правовых и нормативно-методических документов, включающих политику безопасности, инструкции пользователя и администратора и ряд других необходимых документов.

Рис. 4 Основные этапы работ по внедрению комплексной системы обеспечения информационной безопасности (КСИБ)

Защита систем класса ERP

В настоящее время большое число российских предприятий решают задачу автоматизации бизнес-процессов процессов путём использования информационных технологий. В качестве базового инструмента всё больше применяются так называемые ERP-системы (ERP – Enterprise Resource Planning) или системы планирования ресурсов предприятия. Представляют они собой набор специализированного программного обеспечения, позволяющий автоматизировать планирование, учёт, анализ, контроль и управление основными бизнес-процессами предприятия.

Однако эффективность внедрения и дальнейшей эксплуатации любой ERP-системы во многом зависит от того, насколько она защищена от возможных угроз информационной безопасности, которые могут быть связаны с нарушением конфиденциальности, целостности или доступности информационных ресурсов, обрабатываемых средствами ERP-системы. Для защиты от указанных угроз компания предлагает комплексное организационно-техническое решение по обеспечению информационной безопасности ERP-систем Oracle eBusiness Suite (OeBS) и SAP R/3.

Описание решения

Предлагаемое решение обеспечивает:

- криптографическую защиту конфиденциальной информации, передаваемой между клиентской и серверной частью ERP-системы;

- защиту от сетевых атак, которые могут быть направлены на ресурсы сервера ERP-системы;
- защиту от возможной утечки конфиденциальной информации, хранящейся в ERP-системе.

Комплексное решение компании предполагает одновременное использование следующих подсистем защиты:

- подсистемы криптографической защиты, которая использует штатные механизмы ERP-системы для шифрования конфиденциальной информации;
- подсистемы обнаружения сетевых атак, сенсоры которой размещаются в сегменте ERP-системы и обеспечивают обнаружения и блокирование вторжений злоумышленников;
- подсистемы антивирусной защиты, которая размещается на рабочих станциях и на некоторых серверах ERP-системы;
- подсистемы анализа защищённости, предназначенной для своевременного выявления и устранения уязвимостей программного обеспечения ERP-системы;
- подсистемы межсетевого экранирования, предназначенной для блокирования потенциально-опасных пакетов данных, поступающих к серверам ERP-системы;
- подсистемы защиты от утечки конфиденциальной информации, предназначенной для контроля доступа пользователей к внешним портам компьютера.

В общем виде схема размещения средств защиты ERP-системы приведена ниже.

Рис 5. Схема размещения средств защиты ERP-системы

Компоненты решения

Решение по защите ERP-системы базируется на следующих программных продуктах:

- подсистема обнаружения атак базируется на продукте *ISS RealSecure* или *Форпост* компании РНТ, а также программном продукте *Cisco Security Agent*;
- подсистема защиты от вирусов реализуется на базе продуктов *Dr. Web, Microsoft Antigen, Symantec* или *TrendMicro*;
- подсистема анализа защищённости основывается на программном продукте *Xspider* или *ISS Internet Scanner*;
- подсистема сетевого экранирования реализуется на основе продуктов *CheckPoint FW-1* и *Cisco PIX*;

подсистема защиты от утечки конфиденциальной информации базируется на продукте *DeviceLock*, который выполняет функции управления

доступом пользователей к внешним портам, включая USB, LPT, COM, FireWire, BlueTooth и др.

Защищённое информационное взаимодействие через сеть Интернет

В настоящее время Интернет предоставляет возможность использовать удобный и недорогой способ организации информационного взаимодействия между удалёнными подразделениями предприятия. Вместе с тем, использование сети Интернет в качестве среды передачи информации приводит к необходимости обеспечения защиты от следующих основных видов угроз безопасности:

- угрозы нарушения конфиденциальности передаваемой информации посредством её несанкционированного раскрытия;
- угрозы нарушения целостности передаваемых данных посредством их искажения;
- угрозы блокирования канала связи посредством проведения сетевых атак на пограничные коммуникационные узлы системы.

Для защиты от рассмотренных угроз компания предлагает комплексное техническое решение по обеспечению защищённого информационного взаимодействия через сеть Интернет.

Описание решения

Предлагаемое решение обеспечивает:

- криптографическую защиту информации, передаваемую через сеть Интернет;
- защиту от атак из сети Интернет, направленных на блокирование информационного канала связи.

Комплексное решение компании предполагает одновременное использование следующих подсистем защиты:

- подсистемы криптографической защиты, которая обеспечивает конфиденциальность и контроль целостности передаваемой информации посредством её шифрования;
- подсистемы защиты от сетевых атак.

Решение базируется на технологии виртуальных частных сетей VPN (Virtual Private Networks), позволяющей организовать защищённый туннель передачи информации через сеть Интернет. Виртуальная частная сеть представляет собой совокупность сетевых соединений между несколькими криптошлюзами, по которым информация передаётся в защищённом виде. При этом криптошлюзы устанавливаются в точках подключения автоматизированной системы предприятия к сети Интернет. Помимо функций шифрования данных криптошлюзы также обеспечивают возможность фильтрации потенциально опасных пакетов данных, а также функции обнаружения внешних атак.

В общем виде схема размещения средств защиты приведена ниже.

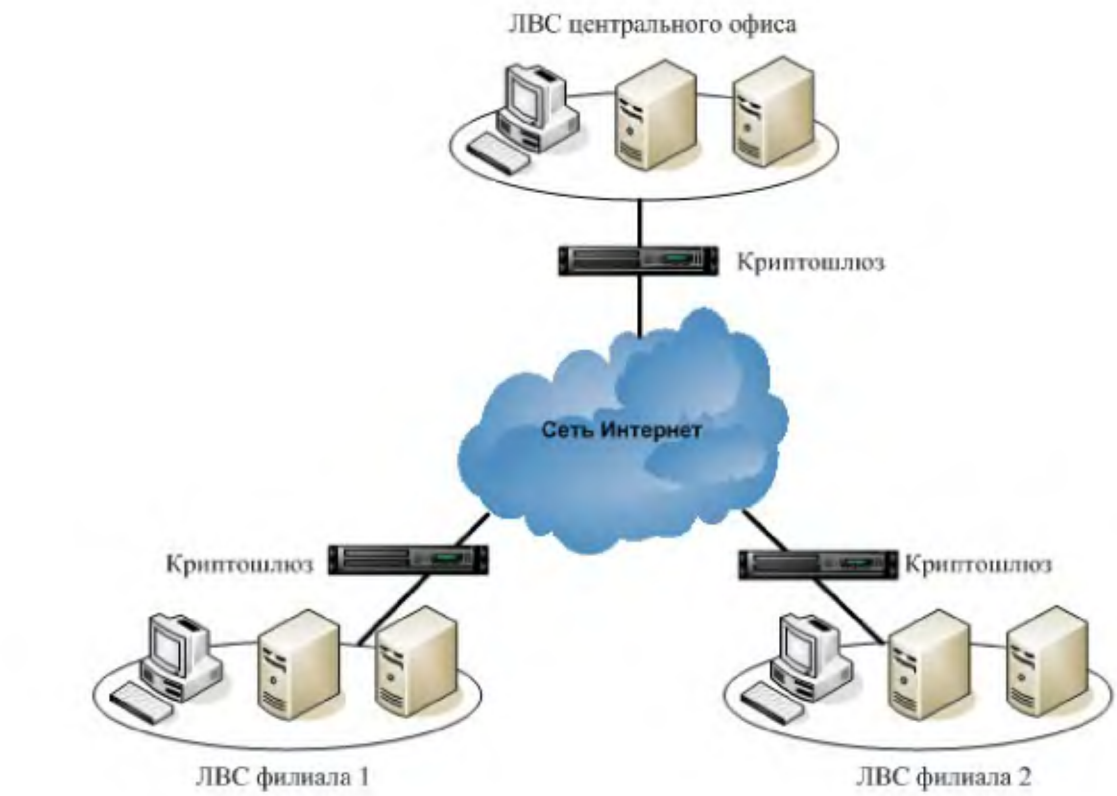


Рис 6. Схема построения виртуальной защищённой сети

Компоненты решения

Решение может базироваться на криптошлюзах *Континет* компании «Информзащита» или системах *ViPNet Координатор* компании «Инфотекс». Данные программные продукты реализуют возможность шифрования информации в соответствии с ГОСТ 28147-89.

Защищённый доступ к сети Интернет

В настоящее время Интернет является необходимым элементом в работе автоматизированной системы практически любой компании. Сеть Интернет используется для отправки электронной почты, поиска необходимой информации, взаимодействия с удалёнными партнёрами и др. Вместе с тем, Интернет является источником большого количества угроз информационной безопасности, таких как компьютерные вирусы и сетевые атаки. Для обеспечения защиты от угроз данного типа компания предлагает комплексное техническое решение по организации безопасного доступа к ресурсам сети Интернет.

Описание решения

Предлагаемое решение по организации защищённого доступа к сети Интернет обеспечивает:

- защиту от компьютерных вирусов и другого вредоносного программного обеспечения, которое может проникнуть в систему компании из сети Интернет;
- защиту от внешних сетевых атак, направленных на информационные ресурсы компании;
- мониторинг и аудит доступа пользователей к ресурсам сети Интернет.

Комплексное решение компании предполагает одновременное использование следующих подсистем защиты:

- подсистемы межсетевого экранирования, выполняющей функции фильтрации потенциально опасных пакетов данных, поступающих из сети Интернет;
- подсистемы защиты от вирусов, обеспечивающей сканирование всего входящего и исходящего сетевого трафика на предмет наличия вредоносного программного обеспечения;
- подсистемы обнаружения атак, предназначенной для своевременного выявления попыток вторжения из сети Интернет;
- подсистемы защиты рабочих станций пользователей от сетевых атак;
- подсистемы мониторинга, выполняющей функции регистрации и ограничения доступа пользователей к ресурсам сети Интернет.

Схема размещения средств защиты показана на рисунке.

Компоненты решения

Решение по защите Интернет-портала базируется на следующих программных продуктах:

- подсистема межсетевого экранирования реализуется на основе межсетевых экранов CheckPoint FW-1 и Cisco PIX;
- подсистема обнаружения атак базируется на программном продукте *ISS RealSecure* или *Proventia*;
- подсистема защиты от вирусов реализуется на базе программных продуктов Dr.Web, Sophos, Symantec или Trend Micro;
- подсистема защиты раочих станций пользователей реализуется на основе персонального сетевого экрана Agnitum Outpost или программного продукта Cisco Security Agent;
- подсистема мониторинга доступа создаётся на основе программного продукта *MIMESweeper* компании ClearSwift.

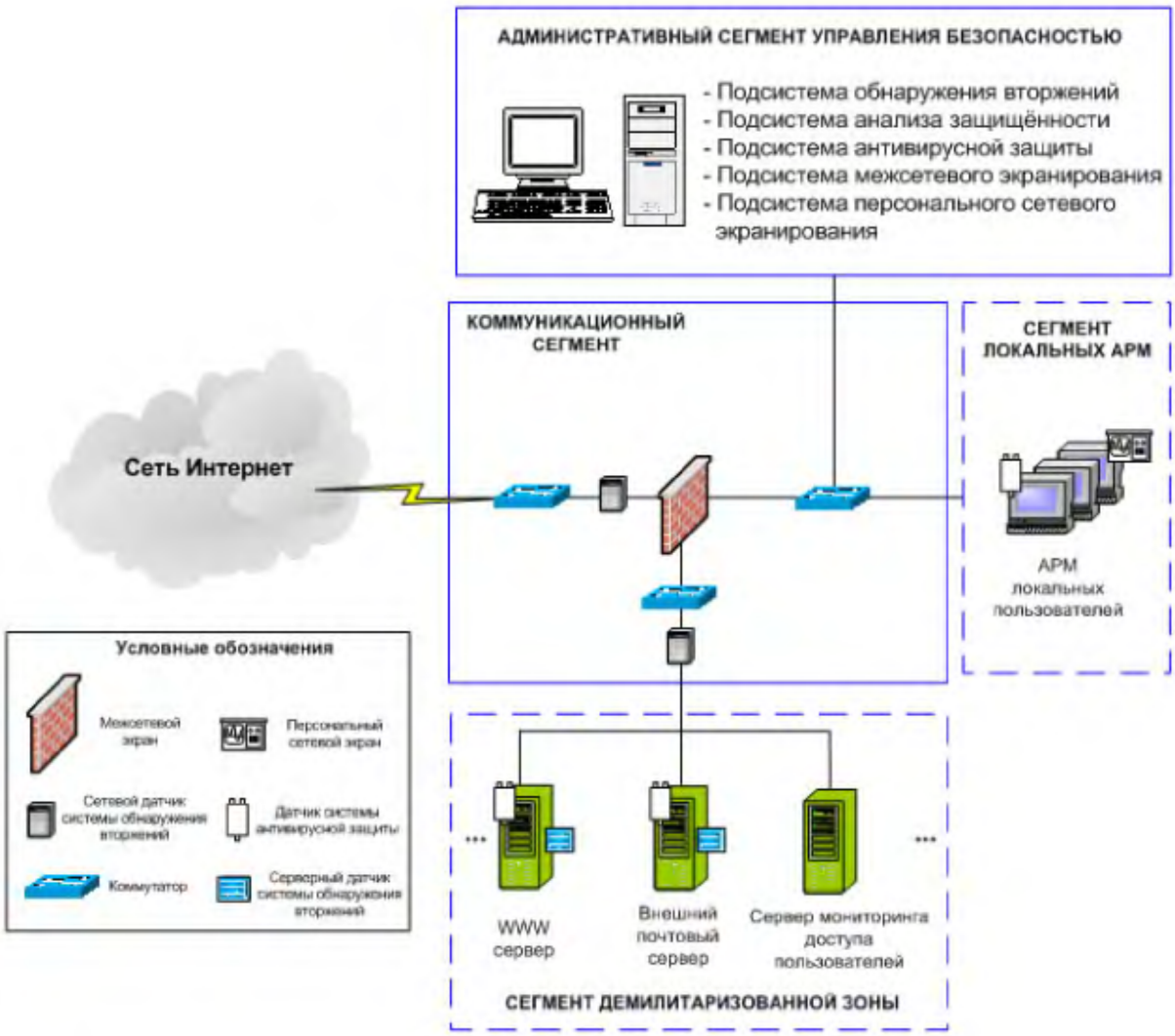


Рис. 7 Схема размещения средств защиты в ЛВС компании

Продукты для предприятий и организаций

- **Защита рабочих станций**
  - Антивирус Dr.Web для Windows
  - Антиспам Dr.Web для Windows
  - Dr.Web Security Space
  - Dr.Web Бастион для Windows
  - Dr.Web для Mac OS X
  - Антивирус Dr.Web для Windows + сервер централизованного управления
  - Антивирусные консольные сканеры Dr.Web для Unix/DOS/OS/2/Windows
  - Антивирус Dr.Web для МСВС (сканер)
  - Sophos Anti-Virus SBE 2.0 (централизованно устанавливаемая и управляемая антивирусная защита для рабочих станций, ноутбуков и файловых серверов)
  - Sophos Computer Security SBE 2.0 (комплексная антивирусная защита рабочих станций, ноутбуков и файловых серверов; в решение включен централизованно устанавливаемый и управляемый сетевой экран для рабочих станций)
  - Sophos Security Suite SBE 2.0 (защита рабочих станций в составе комплекта защиты от вирусов, спама, adware, spyware и потенциально нежелательных сообщений

почтовых и файловых серверов, рабочих станций и ноутбуков; в решение также включен централизованно устанавливаемый и управляемый сетевой экран для рабочих станций)

- Sophos Endpoint Security and Control
- Symantec AntiVirus Corporate Edition (корпоративная защита от вирусов и мониторинг через единую консоль управления)
- Symantec Client Security with Groupware Protection (защита от вирусов, программ-шпионов, хакеров и спама путем обеспечения безопасности настольных компьютеров, файловых серверов и почтовых серверов от угроз)
- Trend Micro OfficeScan Corporate Edition (комплексная защита для корпоративного настольного ПК)
- ESET NOD32 Business Edition
- ESET NOD32 Smart Security Business Edition
- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security
- Avira AntiVir Premium Security Suite
- Avira AntiVir Premium
- Avira AntiVir Professional
- Персональный сетевой экран ViPNet Personal Firewall
- Персональный сетевой экран Outpost Firewall Pro
- Система прозрачного шифрования дисков ViPNet Safe Disk
- Программа шифрования файлов и каталогов ViPNet DISCguise
- Офисный сетевой экран ViPNet Office Firewall (серверное решение)
- Офисный сетевой экран Outpost Office Firewall
- Резервное копирование и восстановление данных Acronis True Image Echo Workstation
- Резервное копирование и восстановление данных Acronis True Image Echo Enterprise Server
- Управление жестким диском Acronis Disk Director Suite 10.0
- DeviceLock для Windows NT/2000/XP - средство контроля доступа к дисководам, CD-ROMам и портам

Secret Disk NG - система защиты конфиденциальной информации

Офисный сетевой экран Outpost Office Firewall

Outpost Office Firewall защищает Ваш офис от всех известных Интернет-угроз. Программа приступает к защите с момента установки, контролируя сетевой трафик при помощи автоматического запуска Outpost Client Firewall на выбранных рабочих станциях всей корпоративной сети. Использование признанной технологии Outpost Firewall technology позволяет клиентскому брандмауэру контролировать весь трафик, таким образом создается высокий уровень защиты Вашей компании.

Возможности Outpost Office Firewall гарантируют Вашей компании высокий уровень безопасности:

Безопасность

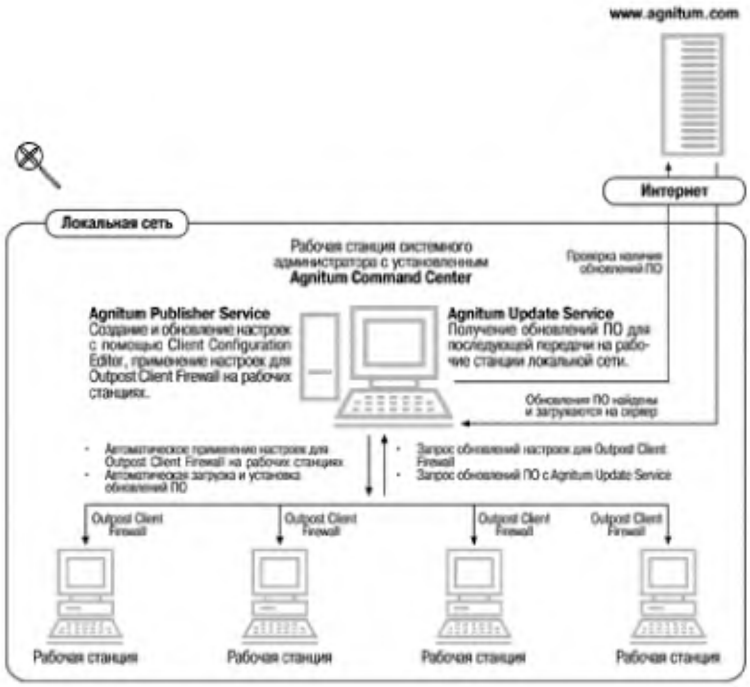
- Защищает все или выбранные рабочие станции в сети;
- Автоматически предотвращает и сообщает о различных Интернет-атаках против рабочих станций пользователей;
- Анализирует входящую почту на предмет опасных вложений;
- Не допускает работу вирусов и "Троянский коней" от имени доверенного приложения.

Контроль

- Позволяет управлять защитой каждой рабочей станции с центральной консоли;
- Позволяет быстро изменять конфигурацию брандмауэра любой рабочей станции для того, чтобы она соответствовала политике безопасности компании;
- Распространяет созданные или измененные конфигурации брандмауэра на рабочие станции пользователей;
- Отслеживает всю сетевую активность рабочих станций.

Простота в использовании

- Обеспечивает простую массовую установку и настройку брандмауэра на рабочие станции в сети;
- Обеспечивает применение новых конфигураций без перезагрузки рабочей станции;
- Консоль не требует установки на сервере или контроллере домена;
- Имеет знакомый пользовательский интерфейс.



Системные требования:

Intel Pentium 233 и выше
Поддержка следующих операционных систем:

- Рабочая станция: Windows 98/ME/2000/ Server 2003/XP;
- Рабочая станция системного администратора: Windows 2000/Server 2003/XP

RAM: 64MB и выше
20Mb свободного места на жестком диске

Возможности Outpost Office Firewall

Outpost Office Firewall обладает необходимыми возможностями для обеспечения высокого уровня защиты Вашей компании.

Безопасность и конфиденциальность

- Защищает все или выбранные рабочие станции в сети
  Развертывая в корпоративной сети клиентскую часть брандмауэра, Outpost Office Firewall защищает Ваш офис от всех известных опасностей в Интернет.
- Клиентская часть брандмауэра основана на признанном Outpost Firewall
  Каждая рабочая станция в Вашей сети прочно защищена с помощью Outpost Firewall, мирового лидера среди брандмауэров.
- Режим невидимости скрывает присутствие компьютера пользователя в сети
  Находясь в режиме невидимости, пользователь является невидимым для

атакующего, что снижает вероятность стать жертвой хакера или "Троянского коня".

- Автоматически предотвращает различные Интернет-атаки против компьютера пользователя и сообщает о них
  Детектор атак обнаруживает и блокирует все известные Интернет-атаки, обеспечивая надежную защиту от вторжения хакеров.
- Анализирует входящую почту на предмет опасных вложений
  Модуль "Фильтрация почтовых вложений" переименовывает подозрительные вложения, предотвращая случайное открытие пользователем вредоносных файлов и защищая его компьютер от вирусов и червей.
- Обеспечивает защиту от проникновения злоумышленников в скрытые лазейки системы
  Брандмауэр реализует защиту от новейших ликтестов, обеспечивая полную безопасность компьютера пользователя, а также предотвращая утечку частной информации.
- Не допускает работу вирусов и Троянский коней от имени доверенного приложения
  Контроль компонентов отслеживает компоненты каждого приложения, запущенного на компьютере пользователя. Контроль скрытых процессов защищает доверенные приложения от запуска опасных для системы программ. Технология "Open Process Control" предотвращает изменение памяти процесса злонамеренными процессами.
- Поддерживает конфиденциальность пользователей в сети, защищает их от вредоносного содержимого web-сайтов
  Модуль "Интерактивные элементы" управляет активным содержимым web-сайтов, которое может нанести вред системе и защищает историю посещений пользователя, гибко блокируя referrers и файлы cookie. Модуль "Реклама" экономит время и трафик пользователя, удаляя рекламные объявления с посещаемых сайтов. Модуль "Содержимое" позволяет блокировать посещаемые пользователем web-страницы с нежелательным содержимым.

Контроль и Управляемость

- Позволяет управлять защитой каждой рабочей станции с центральной консоли
  Командный центр Agnitum позволяет управлять брандмауэрами, установленными на каждой рабочей станции, отслеживать их работу и устранять проблемы с одного компьютера-консоли, экономя Ваше время и усилия.

- Централизованные обновления уменьшают объем используемого в Вашей сети Интернет-трафика
  Agnitum Update Service позволяет назначить время загрузки файлов последних обновлений и установить их на все рабочие станции одновременно. Это существенно снижает нагрузку на сеть.
- Позволяет быстро изменять конфигурацию брандмауэра любой рабочей станции для того, чтобы она соответствовала политике безопасности компании
  Редактор конфигурации позволяет быстро создавать и изменять конфигурацию брандмауэра, используя знакомый интерфейс Outpost Firewall.
- Возможность перезаписать сделанные пользователем изменения в настройках брандмауэра
  Дает возможность перезаписи изменений, сделанных пользователем в настройках своего брандмауэра.
- Распространяет созданные или измененные конфигурации брандмауэра на рабочие станции пользователей
  Редактор конфигурации позволяет автоматически распространять конфигурации брандмауэра с центральной консоли и легко переключаться между различными конфигурациями.
- Отслеживает всю сетевую активность рабочих станций
  Сетевой монитор клиентской части брандмауэра обнаруживает запросы приложений на доступ к сети и позволяет пользователю быстро и адекватно отреагировать с помощью всего лишь нескольких нажатий кнопок мыши.
- С помощью групповых политик Active Directory Вы имеете возможность развертывания и администрирования клиентских брандмауэров на всех компьютерах домена (в том числе, и находящихся в удаленных офисах).

Легкость в установке и использовании

- Обеспечивает простую массовую установку и настройку брандмауэра на рабочие станции в сети
  Вы можете использовать групповые политики Windows для автоматической установки клиентской части брандмауэра в сети.
- Консоль не требует установки на сервере или контроллере домена
  Инструменты управления Outpost Office Firewall могут быть установлены на любой отведенной под эти цели рабочей станции.
- Имеет знакомый пользовательский интерфейс
  Основной инструмент управления выполнен в виде оснастки Консоли

управления (MMC). Клиентская часть брандмауэра наследует настройки Outpost Firewall, делая процесс конфигурации брандмауэра легким и быстрым.

- Обеспечивает применение новых конфигураций без перезагрузки рабочей станции

  Настройки клиентской части брандмауэра применяются «на лету» по запросу компьютера пользователя и не требуют его перезагрузки.

Использует встроенные технологии Windows

Outpost Office Firewall использует такие знакомые администраторам технологии, как Консоль управления (MMC), групповые политики (Group Policy) и другие, снижая затраты на обучение персонала.

Для защиты локальной сети офиса, подключенной к Internet, можно использовать программные продукты компании ЭЛВИС+ ряда ЗАСТАВА. На шлюз устанавливается ЗАСТАВА-Офис, на сервер сети – ЗАСТАВА-Сервер, на рабочии станции – ЗАСТАВА-Клиент.